**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| **PATRICK COLLINS, INC.,** | **:** | **CIVIL ACTION** |
| **Plaintiff** | **:** | |
| | **:** | |
| **vs.** | **:** | **NO. 12-3146** |
| | **:** | |
| **JOHN DOES 1-11, 13-18, and 20-23,**[1] | **:** | |
| **Defendants** | **:** | |

**M E M O R A N D U M**

**STENGEL, J.** **January 31, 2013**

Plaintiff Patrick Collins, Inc., originally brought this action against twenty-three John Doe defendants alleging that they had infringed its copyright in the motion picture entitled "Busty Construction Girls" by reproducing and distributing it over the internet using a peer-to-peer file-sharing protocol called BitTorrent. The John Does are identified only by internet protocol ("IP") addresses corresponding to the internet connections alleged to have been used to infringe the plaintiff's copyright.

I granted the plaintiff's earlier motion for leave to file third-party subpoenas on the Internet Service Providers ("ISP") servicing the IP addresses identified in the complaint to help determine the identity of the defendants. The plaintiff reached a settlement with two of the defendants, and voluntarily dismissed its claims against them.

John Doe #13 filed a *pro se* "joint motion to sever defendants and/or quash the subpoena." Because the joinder of the John Doe defendants is proper and quashing the subpoena would be inappropriate at this time, I will deny the motion.

[1] The plaintiff voluntarily dismissed its claims against Defendants John Doe #12 and #19. See Documents #8 and #10.

## I. BACKGROUND

BitTorrent is one of the most common peer-to-peer file sharing protocols, i.e., set of computer rules, used for distributing large amounts of data. See Compl. ¶ 14. It has been estimated that users using the BitTorrent protocol on the internet account for over a quarter of all internet traffic. Id. Its popularity stems from its ability to distribute a large file without creating a heavy load on the source computer and network. To reduce the load on the source computer, the BitTorrent protocol allows users to join a "swarm" of host computers to download and upload from each other simultaneously. Id. at ¶ 15.

Here, it is alleged that each defendant installed a BitTorrent "Client" onto his computer. A "Client" is a software program that implements the BitTorrent protocol. Id. at ¶¶ 16-17. Once installed, the BitTorrent Client serves as the user's interface during the process of uploading and downloading data using the BitTorrent protocol. Id. at ¶ 18. A BitTorrent user that wants to upload a new file, known as an "initial seeder," starts by creating a "torrent" descriptor file using the Client he installed onto his computer. The Client takes the target computer file, the "initial seed," here the "Busty Construction Girls" movie, and divides it into identically sized groups of bits known as "pieces." Id. at ¶¶ 19-20. The Client then gives each one of the pieces a random and unique alphanumeric identifier known as a "hash" and records these hash identifiers in the torrent file. When other users, known as "peers," receive a particular piece, the hash identifier for that piece is compared to the hash identifier recorded in the torrent file for that piece. Thus, the hash identifier works like an electronic fingerprint to identify the source of the piece and that the piece is authentic and uncorrupted. Id. at ¶¶ 21-22.

When peers download the torrent file, the BitTorrent protocol signals that those peers are seeking to download the original file, and the seeder begins to distribute pieces

to those users. Once a peer has downloaded a piece, it serves as a source of that piece to other peers possessing the torrent and seeking to download the original file. When a peer has downloaded all of the pieces, the client program continues to distribute the file. In this way, the initial seeder and peers serve to share and distribute the original file in an activity known as a "swarm." See Compl. ¶¶29-32.

## II. DISCUSSION

### A. Motion to Sever

John Doe #13 argues that the plaintiff has improperly joined twenty-three defendants in this action because the defendants' involvement arose from distinctly separate transactions that involved separate sets of facts and defenses. Because there is no nexus between him and the other defendants, he requests that I "sever and dismiss all the defendants." I disagree and will deny his request.

Federal Rule of Civil Procedure 20(a)(2) permits joinder of numerous defendants in one action if "any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and any question of law or fact common to all defendants will arise in the action." See FED.R.CIV.P. 20(a).

The Court of Appeals for the Third Circuit has not directly interpreted Rule 20(a), but it has held that events comprising the same transaction or occurrence bear a "logical relationship" to one another and involve the same factual issues or the same factual and legal issues. Transamerica Occidental Life Ins. Co. v. Aviation Office of Am., Inc., 292 F.3d 384, 390 (3d Cir. 2002). Thus, the impulse under the Federal Rules is "toward entertaining the broadest possible scope of action consistent with fairness to the parties; joinder of claims, parties, and remedies is strongly encouraged." Hagan v. Rogers, 570

F.3d 146, 152 (3d Cir. 2009) (quoting United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 724 (1966)). Rule 20(a)'s purpose is to promote trial convenience and expedite the final determination of disputes, thereby preventing multiple law suits. See Al Daraji v. Monica, No. 07-cv-1749, 2007 U.S. Dist. LEXIS 76205, *10 (E.D. Pa. Oct. 12, 2007). The rule is designed to promote judicial economy and reduce inconvenience, delay, and added expense. Id.

Here, the plaintiff alleges that each of the defendants participated in the same swarm, sharing and distributing the plaintiff's motion picture. See Compl. ¶ 33. The plaintiff retained a computer investigation firm, which used forensic software to track and identify BitTorrent activity involving a specific copy of the movie that was identified by its own "Unique Hash Number." Id. ¶¶ 36-39. The investigation identified twenty-three IP addresses, corresponding to the defendants here, that participated in the same swarm by transmitting a separate piece of this version of the movie using the BitTorrent protocol. Each IP address connected to a server established by the plaintiff's investigator and transmitted a piece of the same copy of a file constituting the plaintiff's movie. Id. ¶¶ 40-41. The pieces are then reassembled resulting in a fully playable digital motion picture of the plaintiff's work. Id. By participating in the same swarm, the defendants are each alleged to have directly infringed the plaintiff's copyright in the movie and to have "induced, caused, or materially contributed to the infringing conduct" of the other defendants. Id. ¶ 55.

The plaintiff's allegation that the defendants downloaded and shared the same file, were part of the same swarm, and are contributorily liable for each other's infringement is sufficient to establish that the claims against each defendant are logically related and arise out of the same transaction, occurrence, or series of transactions and occurrences.

Further, the infringement claims contain common questions of law and fact regarding the defendants by virtue of the use of BitTorrent to transmit the same copy of the plaintiff's motion picture. Thus, joinder is appropriate at this stage of the litigation. Accordingly, I will deny Defendant John Doe #13's motion to sever without prejudice.[2]

**B. Motion to Quash**

John Doe #13 next argues that the subpoena should be quashed because the plaintiff does not have legal legitimacy to request early discovery of the defendants' identities. He insists that this information infringes upon his privacy interests as protected under the First Amendment of the United States Constitution. Again, I must disagree.

A court *must* quash a subpoena under certain circumstances, including when it subjects a person to undue burden. See FED.R.CIV.P. 45(c)(3)(A)(iv) (emphasis added). A court *may* quash or modify a subpoena if it requires disclosure of "a trade secret or other confidential research, development, or commercial information" or requires a nonparty to "incur substantial expense." See FED.R.CIV.P. 45(c)(3)(B)(i) and (iii) (emphasis added). It may also modify a subpoena if the serving party "shows a substantial need for the testimony or material that cannot otherwise be met without undue hardship." *See* Fed. R. Civ. P. 45(c)(3)(C).

The defendant's arguments do not raise valid grounds for quashing the subpoena served on Comcast. Proceeding with discovery to obtain the identity of the defendants so that they may be served is proper and within the scope of permissible discovery. See

[2] Rule 21 of the Federal Rules of Civil Procedure grants the court authority to revisit the issue of misjoinder at any point in an action, either by motion or *sua sponte*. With this procedural protection in mind, I will deny the motion to sever the defendant without prejudice to his ability to raise the issue of misjoinder at a later time.

Blakeslee v. Clinton County, 336 F. App'x 248, 250 (3d Cir. 2009) (discovery for the purpose of identifying John Doe defendants is permissible). Moreover, the Federal Rules of Civil Procedure permit parties to obtain discovery of "the identity and location of persons who know of any discoverable matter." See FED.R.CIV.P. 26(b)(1).

The plaintiff moved for leave to serve discovery prior to a Rule 26(f) conference. See Document #4. At that time, the plaintiff showed that a subpoena seeking the subscriber information associated with the allegedly infringing IP addresses would be the only way for the plaintiff to identify the proper defendants in this case and proceed with its claims against them. The information sought is thus highly relevant to the plaintiff's claims.

Defendant John Doe #13 also argues that the subpoena must be quashed because disclosure of his identity is violative of his First Amendment right to engage in anonymous online communication. The Constitution protects the right to engage in anonymous communication, and that protection extends to the internet. See Reno v. ACLU, 521 U.S. 844, 870 (1997). The First Amendment is implicated by civil subpoenas seeking the identify of anonymous individuals. NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958). However, anonymous speech is not entitled to absolute protection, particularly if the speech consists of copyright infringement. Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555-56, 569 (1985).

The Court of Appeals for the Third Circuit has not yet articulated a standard for balancing the need for discovery against the right to anonymous speech. Courts around the country have applied standards that vary according to the nature of the protected speech and the showing required to overcome that protection. One such test was adopted

by the Court of Appeals for the Second Circuit. Arista Records LLC v. Doe, 604 F.3d 110, 119 (2d Cir. 2010). The test analyzes the following five factors to determine whether the need for disclosure of an individual's identity outweighs the right to anonymity where the speech alleged is copyright infringement: (1) a *prima facie* claim of infringement; (2) the specificity of the information sought from the ISP; (3) a lack of alternative means of obtaining that information; (4) a "central need" for the information in order to bring the claim; and (5) the expectation of privacy held by the objecting party. Id. (quoting Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp. 2d 556, 564-567 (S.D.N.Y. 2004)). Finding that the information sought by the plaintiff's subpoena was necessary to advance its claim, the court denied the motion to quash. Id. at 124.

Here, the complaint makes a *prima facie* claim of copyright infringement which requires "(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original." Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 361 (1991). The plaintiff alleges that it owns the copyright in "Busty Construction Girls" and that the defendants, through the use of BitTorrent, connected to the plaintiff's investigative server and copied elements of the movie.

Next, the subpoena is specific enough to give rise to a reasonable likelihood that information facilitating service upon proper defendants will be disclosed if the ISP's comply. The subpoena seeks the name, address, telephone number, e-mail address, and "Media Access Control" address, which identifies the specific equipment using the IP address, of the subscriber to whom the served ISP assigned the specific IP addresses at the dates and times of the alleged infringement. Although the provision of this

information may not directly identify the proper defendants, it is sufficiently tailored to lead to the identification of those individuals. The first and second factor thus weigh against quashing the subpoena.

The third and fourth factors of the test also weigh against quashing the subpoena. The plaintiff has previously shown that obtaining the subscriber information possessed by the ISP's is the only reasonable means of discovering the identity of the subscribers whose IP addresses were used to commit the alleged infringement here.

Finally, courts analyzing the expectation of privacy possessed by internet users engaging in online file-sharing have concluded that such expectation is at most minimal because those individuals have already voluntarily given up certain information by engaging in that behavior. See Malibu Media, LLC v. Doe, 2012 U.S. Dist. LEXIS 105768, *20-21 (E.D. Pa. July 30, 2012) (citing Raw Films, Ltd. v. John Does 1-15, 2012 U.S. Dist. LEXIS 41645, at *8 (E.D. Pa. March 23, 2012))(an internet user engaging in peer-to-peer file sharing has a minimum expectation of privacy); Sony Music Entertainment Inc., 326 F. Supp. 2d at 566-567. One court aptly summarized this sentiment by stating that, "it is hard to understand just what privacy expectation he or she has after essentially opening up the computer to the world." Malibu Media, LLC, 2012 U.S. Dist. LEXIS 105768, *20-21 (quoting In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 267 (D.D.C. 2003) *rev'd on other grounds*, Recording Indus. Ass'n of America Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003)). This is especially true because the internet subscribers have already voluntarily conveyed their subscriber information, i.e., name, address, and phone number, to their internet service

provider." Malibu Media, 2012 U.S. Dist. LEXIS 105768, at *8. This expectation of privacy is even lower where the alleged transmissions include copyright protected works. Sony Music Entertainment Inc., 326 F. Supp. 2d at 566-567.

Here, the defendants have already disclosed their personal information to their ISP's in order to set up their internet accounts. It is unreasonable, then, to assert a claim of privilege or privacy which would serve as a basis for quashing a subpoenas under Rule 45. Even if the defendants retained a reasonable expectation of privacy in their subscriber information, that interest is substantially outweighed by the need to disclose it so that the plaintiff may proceed with bringing what appear to be non-frivolous claims of copyright infringement that cannot be advanced by other means.

Accordingly, because I find that the information sought in the subpoena is relevant to the plaintiff's claims, and under the circumstances, the plaintiff's right to pursue its claims of infringement by means of discovering subscriber information outweighs the defendant's asserted rights to remain anonymous in connection with the alleged infringing activity, I will deny the defendant's motion to quash the subpoena.

An appropriate Order follows.